can receive the completed ballot, and then either scan in or otherwise convert the votes on the paper ballot into digital votes, add those votes to the blockchain, certify the voter has voted, and ensure that the digital votes are added to the vote tallies of the candidates for election on the ballot.

[0047] FIG. **1** depicts exemplary system architecture for a blockchain management portion of a blockchain powered vote by mail system. The exemplary system architecture **100** contains a blockchain access layer **101**. Blockchain access layer **101** provides access to a blockchain (not shown) for the various system architecture components. It also can coordinate all of the non-blockchain related functions of the system. In some embodiments, the blockchain access layer **101** can comprise numerous servers running separate blockchain access layer software with a load balancer balancing the demand between the servers. In some embodiments, the blockchain is a digital ledger in which state changes are recorded. In some embodiments, the accuracy of the blockchain is ensured through the use of cryptographic functions such that previous entries in the ledger cannot not be altered without the alteration of all subsequent parts of the ledger. In some embodiments, the blockchain is separated into "blocks" of data, wherein each block contains a hash of the data of the previous block. In some embodiments, the blockchain is separated into different blocks based upon the number of entries on the digital ledger or on the amount of data stored in the digital letter. For example, each block could contain 10, 100, 1,000 or 1,000,000 ledger entries or other number of entries. Each block could also contain 10, 100, 1,000 or 1,000,000 Mb of data, or other amount of data.

[0048] In some embodiments, the blockchain can be used to defeat fraud because cryptographic functions which ensure the accuracy of the blockchain prevent bad actors from altering the blockchain. In some embodiments, the blockchain can also be used by voters, election officials, auditors, or other authorized interested parties, to check to make sure their votes were received and counted because the blockchain provides an easily accessible and robust method of recording voting actions in an unalterable way.

[0049] The embodiments of the data stored on the blockchain in the exemplary system architecture are discussed further below. In some embodiments, the blockchain is based on the Ethereum open software platform or other similar platforms. In some embodiments, the platform is a Turing complete blockchain protocol. In some embodiments, the blockchain access layer uses software "contracts" that write data to the blockchain when certain conditions are met. In some embodiments, the "contracts" can be used to develop software objects such as those further described below.

[0050] In some embodiments, blockchain access layer **101** is in wired or wireless communications with entities **110** that can interact with the blockchain directly. In some embodiments the entities **110** communicate with the blockchain access layer through a software API (not shown). In some embodiments, this can be REST-API. In some embodiments, the entities comprise a member **111** that can act as a committer on the blockchain. A committer can add validated transactions to the blockchain, thereby writing data to the ledger. In some embodiments, the member **111** can comprise numerous servers running separate member software with a load balancer balancing the demand between the servers. The ledgers can be distributed among member nodes and parity nodes. The nodes can be maintained by various election precincts or districts or election systems. In some embodiments, the blockchain ledger is not publicly distributed, but is distributed among election authorities for a county, state, country, or any combination thereof

[0051] In some embodiments, the entities also include parity authorities **112***a-c*. Parity authorities **112***a-c* act as validators for the transactions entered onto the block, ensuring that the transactions accurately reflect what happened. In some embodiments, the parity authorities **112***a-c* can be used as part of a consensus mechanism known as Proof of Authority (PoA). Instead of using miners to validate and create blocks on the blockchain, PoA relies on a group of nodes referred to as authority nodes or validators contained within the parity authorities. Using a round-robin structure, each authority node gets a time slot per round in which it can create and sign one new block. In case a validator is offline or not responding, it will be skipped. The validator signing a block is called the primary. In some embodiments, at least five authority nodes will be allocated among the parity authorities. In some embodiments, each parity authority can have more than one node. In some embodiments, load balancer can be used to balance the load on the various parity authorities acting as validators.

[0052] In some embodiments, blockchain access layer **101** is also in communication with identity services **130**. In some embodiments, identity services **130** can communicate with the blockchain access layer **101** through a software API. In some embodiments, this can be REST-API.

[0053] Identity services **130** allow the system to confirm voter identity, and to ensure the voters are registered with the system, and to ensure the voters get the correct ballot for the precinct, jurisdiction, municipality, or other government or political division in which the voter is located. In some embodiments, the voters enter credentials, identity proofing documents, and other required documentation into the system through user interface **131**.

[0054] In some embodiments, the blockchain access layer **101** can be in communication with a user interface **131**. In some embodiments, the blockchain access layer **101** can communicate with the user interface **131** through an internet or other software protocol. In some embodiments, this can by Hyper Text Transfer Protocol or Hyper Text Transfer Protocol Secure. The user interface **131** allows the various users of the system, also called participants, to interact with the system. In some embodiments, there are three types of participants who can interact with the system: voters, election registrars, and notaries. Each of these types of users can interact with the system in different ways through the user interface, as described further below.

[0055] Identity services **130** then submits these proofs provided through user interface **131** to various authorities to ensure that the person's identity is confirmed. In some embodiments, these authorities could be the FBI, Equifax, the Social Security Administration, a state department of motor vehicles, or another agency that confirm identities. The identity services **130** can then generate a unique voter ID and a public/private key pair for each voter, store them appropriately, and notify the voter. In some embodiments, the identity services **130** can store the various data in a JSON data structure.

[0056] In some embodiments, the blockchain access layer **101** is in communication with electronic postmark® (ePM) system **132**. In some embodiments, ePM system **132** operates in the manner describe in U.S. Patent Application No.